



**Privacy Impact Assessment
for the
Case and Activity Management System**

Date

August 10, 2007

Contact Point

System Owner: Stephanie Monroe, OCR
Author: Ting-Ting Wang
Office for Civil Rights

U.S. Department of Education

1. What information will be collected for the system (Ex. Name, Social Security Number, annual income, etc)?

The Office for Civil Rights (OCR) utilizes the Case and Activity Management System (CAMS) that contains in-house developed applications, Case Management System (CMS) and Activity Management System (AMS), commercial-off-the-shelf (COTS) software, and Hummingbird Document Management System (DMS). The CAMS collects the complainant's name, address, and phone number, and identifies the specific allegations of discrimination at issue and statements of facts in support of the allegations.

2. Why is this information being collected?

This information is collected to enforce six Federal statutes that prohibit discrimination in education programs and activities that receive Federal financial assistance

3. How will the information be used?

The information is used to manage the OCR caseloads and provide reporting information used in Congressional reports, budget requests, Freedom of Information Act (FOIA) requests, and requests from other government agencies and the general public.

4. Will this information be shared with any other agency or entity? If so, with whom?

The Department of Education (Department) may disclose information contained in a record in this system of records under the applicable routine uses without the consent of the individual if the disclosure is compatible with the purposes for which the record was collected, i.e., enforcing Federal Statutes. Possible disclosures include:

- Disclosure to Congress, Other Agencies, or the Public
- Disclosure to Recipients of Federal Financial Assistance, Witnesses, or Consultants
- Disclosure for Use by Other Law Enforcement Agencies
- Enforcement Disclosure
- Litigation and Alternative Dispute Resolution (ADR) Disclosures
- Freedom of Information Act Advice Disclosure
- Research Disclosure
- Congressional Member Disclosure

These disclosures may be made on a case-by-case basis or, if the Department has complied with the computer matching requirements of the Privacy Act, under a computer matching agreement.

There will be no sharing of information for purposes outside of the above disclosure requirements or for anything other than the primary purpose(s) of collecting the information. Any contractor responsible for the operations of the CAMS is held to the privacy and security requirements of the Department of Education in the handling of information collected through the systems.

5. Describe the notice or opportunities for consent that are provided to individuals about what information is collected and how that information is shared with other organizations. (e.g., posted Privacy Notice).

As the CAMS resides in the Department network and is restricted to OCR access, the Privacy Policy is shared with CAMS users when the information is collected. This is a general policy, which applies to the handling of any information collected in the CAMS. The policy highlights the voluntary nature of information collected, and explains which data elements are necessary for each level of functionality. Complainants are notified that providing the information constitutes consent to all of its uses.

6. How will the information be secured?

The information is secured following the guidance of OMB Circular A-130, "Management of Federal Information Resources," Appendix III, "Security of Federal Automated Information Resources," and Public Law 100-235, "Computer Security Act of 1987." The CAMS resides in the Department network and is in compliance with Department Risk Assessment policy and procedures. The CAMS System Security Plan details the security requirements and describes the security controls that are in place to meet those requirements.

Sensitive data, such as that covered by the Privacy Act, needs to be protected from unauthorized disclosure, modification, and destruction. All printouts that contain Privacy Act data are marked For Official Use Only (FOUO). The following guidelines and procedures have been implemented for protecting CAMS sensitive data and resources.

- Labeling of sensitive data properly (FOUO)
- Using sensitive file covers and folders
- Computers are not left unattended when processing sensitive data or when sensitive data or a critical application system is resident in memory
- Sensitive information is placed out of sight when visitors are present
- Sensitive material is stored in a secure safe or a locked cabinet and material is returned to the safe each evening or during any lunch periods or breaks greater than 30 minutes
- Data is stored in a media storage vault or library with restricted access and is environmentally protected.

7. Is a system of records being created or updated with the collection of this information?

While a System of Records exists for this collection of data, the tool used to collect this type of data was modified. Users are provided notice of rights under the Privacy Act via links to the agency Privacy Act regulations (34 C.R.F. Part 5b) and to the Privacy Act System of Records notice for the Complaint Files and Log, Number 18-08-01 (69 Fed. Reg. 12248 (March 15, 2004.)).